infoexpress

Alcatel·Lucent

Alcatel-Lucent Operating System for OmniSwitch LAN Switches with Integrated CyberGatekeeper Solution

Alcatel-Lucent offers a seamless, secure and scalable enterprise network access control solution through its embedded network security framework. This framework includes a comprehensive security solution for verifying endpoint integrity through host integrity checking (HIC). The solution is the result of integration between InfoExpress CyberGatekeeper and the Alcatel-Lucent OmniSwitch™ 6400 Stackable Gigabit LAN Switch (SGS), the Alcatel-Lucent OmniSwitch 6850 Stackable LAN Switch (SLS) and any edge switches using the Alcatel-Lucent Operating System™ (AOS), Release 6.3.4 or later.

Key features

- Automatically manages the security fitness of endpoints
- Operates independently of authentication mechanism and network access controls
- Integrates endpoint compliance directly with the edge switch
- InfoExpress CyberGatekeeper integration with the Alcatel-Lucent OmniSwitch™ ensures endpoint device security policy compliance with quarantine and remediation as required
- Enhanced security at the network edge with InfoExpress CyberGatekeeper HIC policy server
- Compatible with Microsoft®, Windows®, Mac®, Linux, mobile, PDA
- Captive portal for web-based user authentication with configurable web page
- Agents are permanently installed or provided on-demand
- Dynamic enforcement via access control lists (ACLs), not VLAN or IP address changes
- Central policy management delivers consistent user experience
- Continuous surveillance of endpoint configuration

Key benefits

- Ensures 100 percent of network endpoints are compliant (patch levels, configurations and application settings) or they are quarantined until remediated
- Separates authentication mechanism from security
  - 802.1x not a requirement for HIC
  - Endpoints can be plugged into phones and still be secured
- Will not interfere with existing VoIP deployments
- Keeps rogue devices off the network
- Reduces vulnerabilities – Security solutions, OS and patches are assured to be running and up-to-date
- Lowers help desk costs – Automatic remediation of non-compliant PCs
- Improves security compliance/auditing scorecard
- Reduces risks associated with improperly configured computers
- Integrates with existing patch management solutions to preserve software investments
- Reduces support costs by maintaining standard configurations across desktops

The Alcatel-Lucent OmniSwitch families of Stackable LAN Switches and InfoExpress CyberGatekeeper solution provide enterprise customers with a comprehensive network access control and HIC security layer. Enterprise LAN segments with the OmniSwitch 6400 SGS and the OmniSwitch 6850 SLS running AOS, Release 6.3.4 or later benefit from enhanced authentication and user-profile-enabled network access control. Enterprise LAN segments with third-party switches are protected by InfoExpress CyberGatekeeper Dynamic Access Control (DNAC) technology. Wireless and VPN users are protected by InfoExpress in-line appliances.

Please refer to the InfoExpress CyberGatekeeper data sheet for complete details on the InfoExpress CyberGatekeeper product line.

Through the integrated solution, enterprises ensure endpoint devices are verified to be compliant and healthy when initially connecting to the network. Only those endpoint devices that are compliant with enterprise security policies are allowed access to the production network. Those endpoint devices that fail the HIC are redirected at the switch level by the Alcatel-Lucent

Access Guardian AOS feature, and allowed access only to the remediation servers. The HIC agent (permanently installed or provided on-demand) on the endpoint, in conjunction with the InfoExpress CyberGatekeeper policy server, attempts to update the endpoint. Once compliant with security policies, the endpoint is allowed network access. As long as the endpoint is connected to the network infrastructure, the HIC agent provides continuous surveillance. If the agent detects a violation of the security policies or is disabled or terminated, the policy server will notify the switch, which in turn quarantines the endpoint and allows access only to the remediation servers.

The OmniSwitch 6400 SGS/OmniSwitch 6850 SLS/InfoExpress CyberGatekeeper solution is easy to deploy and maintain, requiring no network changes. Installations can be done in hours compared to those for most network access control solutions that can take weeks or months.

User network profile

When a device initially connects to the enterprise network edge, the OmniSwitch 6400 SGS or the OmniSwitch 6850 SLS authenticates the user/device as defined by its Access Guardian policy. The OmniSwitch 6400 or OmniSwitch 6850 subsequently identifies the corresponding user network profile (UNP), which is a security profile.

UNPs allow the creation of easily defined profiles that are mapped to security policies. A profile may contain network, application, priority, bandwidth and compliancy rules based on a user's role in the organization. The UNP is provided during authentication and rules are enforced immediately by the network switch. During this time, the switch allows the endpoint limited access to the network. Authentication using 802.1X, MAC or web-based methods is not required, but can be added to provide more granular control of the profiles.

Operation

When a user/device connects to an enterprise network with HIC, the endpoint device is required to undergo a verification process. The switch dynamically restricts network access using ACLs, which only allow the endpoint access to the InfoExpress CyberGatekeeper Policy Server and the remediation server(s).

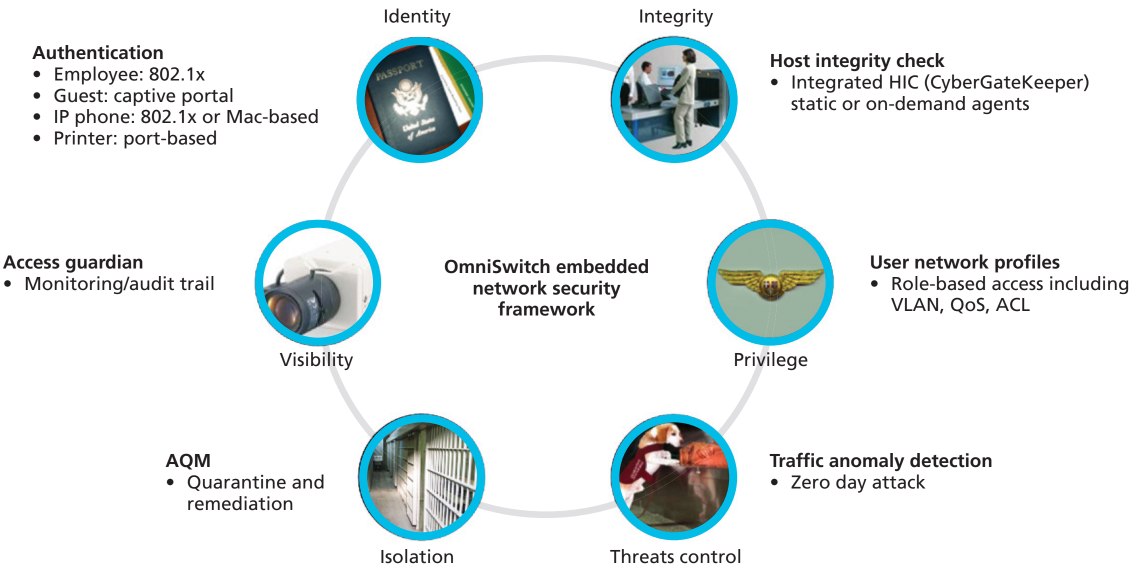
If the endpoint device has a permanent InfoExpress CyberGatekeeper Agent installed, the agent communicates with the InfoExpress CyberGatekeeper Policy Server to assess the endpoint's integrity. The tests to be performed on the endpoint device by both the permanent agent and the web-based on-demand agent are defined on the InfoExpress CyberGatekeeper Policy Server using the InfoExpress CyberGatekeeper Policy Manager. The policy server determines whether the endpoint device has passed or failed the HIC test and directly notifies the edge OmniSwitch 6400 SGS or OmniSwitch 6850 SLS to which the device is connected. Traffic restrictions and redirections are processed by the Alcatel-Lucent Access Guardian AOS feature, which integrates authentication, device compliance and network access control functions directly into the network infrastructure at the switch level.

If the OmniSwitch 6400 SGS or the OmniSwitch 6850 SLS receives a HIC pass status for the specified endpoint device, the switch dynamically applies a new set of ACLs that allow the endpoint device access to the production network.

If the OmniSwitch 6400 SGS or the OmniSwitch 6850 SLS receives a HIC fail status for the specified endpoint device, the switch dynamically applies a restrictive set of ACLs that allow the endpoint to access the remediation servers only.

If the endpoint device does not have a permanent agent installed on it, the user is required to launch a browser that is redirected to a customer-defined

Figure 1. OmniSwitch AOS - Embedded network security framework



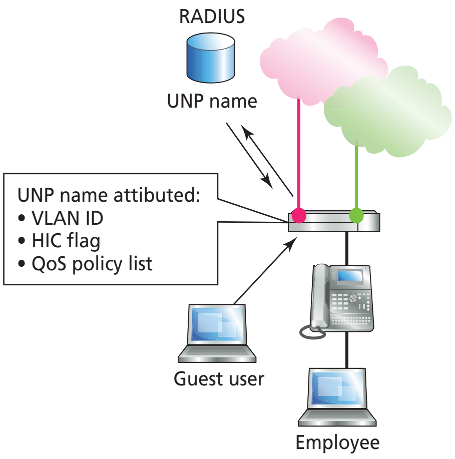
web server. From here the InfoExpress CyberGatekeeper web agent is automatically downloaded onto the end-user's device. This web agent communicates with the InfoExpress CyberGatekeeper Policy Server and performs an integrity assessment. When complete, the agent reports the endpoint's status to the policy server. If the endpoint complies with security policies, it is allowed access to the network. Otherwise it is directed to the remediation server so it can be patched to meet security requirements.

The endpoint HIC test is not a one-time test; it is a periodic and continuous process that provides constant surveillance while the endpoint is connected to the network. If at any time the endpoint device fails the HIC test, its access is automatically restricted to the remediation network. The InfoExpress CyberGatekeeper agent may be pre-installed on Microsoft® Windows®, Mac OS® X, or Linux® operating systems, or the user's web browser can be redirected to a download page to load a web-based on-demand version of the agent.

Easy to deploy

The Alcatel-Lucent/InfoExpress solution is easily deployed. The authentication and HIC redirection are built into the Alcatel-Lucent Access Guardian, which is a function of the AOS, Release 6.3.4. Once turned on, all that is needed is the addition of the InfoExpress CyberGatekeeper Policy Server, the InfoExpress CyberGatekeeper Agent, and the creation of network security policies. No modifications to the network are needed, meaning deployment takes hours instead of days.

Figure 2. User network profile (UNP)



What?

- This feature is to provide the capability to have roles/profiles assigned to users during authentication
- More than just a VLAN
- Eases implementation of central RADIUS configuration
- Scalable deployment with 8 distinct ACL/QoS policy lists

How?

- UNP name is stored in RADIUS and returned to the switch
- The switch maps the UNP name to the actual profile attibutes
- Profiles determine
  - ¬ VLAN ID (mandatory)
  - ¬ HIC flag (optional)
  - ¬ QoS/ACL Policy LIst Name (optional)

Benefits

Simplify network access control management

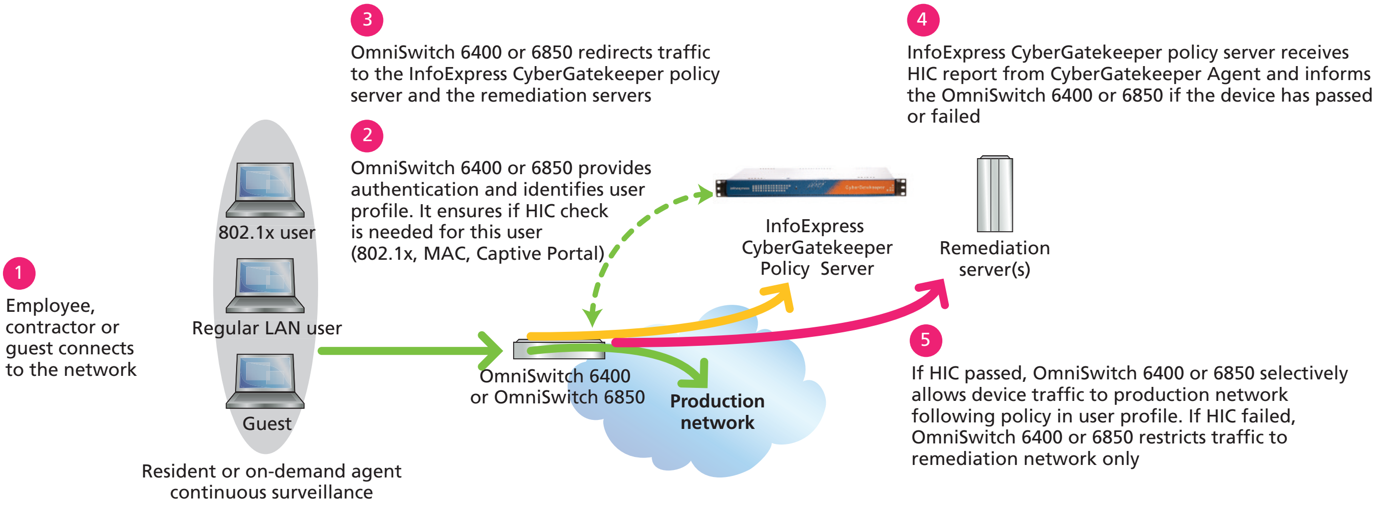
Saves time and money

Once in place, the automated compliancy checking and updating means fewer support calls to apply software upgrades and system patches. In addition, because each endpoint is more secure (endpoint access is restricted at the switch level until compliance is met), there is less chance of a security breach from malware being introduced to the network.

Simplifies network management

The Alcatel-Lucent Access Guardian and InfoExpress CyberGatekeeper simplify network management of endpoints. The edge switch integrates authentication, device compliance and access control functions directly into the hardware. Switch-based security functions allow an administrator to configure, manage and maintain the entire security infrastructure more efficiently and without additional equipment. HIC provided by the InfoExpress CyberGatekeeper simplifies network maintenance by automatically managing the security fitness of endpoints.

Figure 3 OmniSwitch + CyberGatekeeper integration



1 Employee, contractor or guest connects to the network

2 OmniSwitch 6400 or 6850 provides authentication and identifies user profile. It ensures if HIC check is needed for this user (802.1x, MAC, Captive Portal)

3 OmniSwitch 6400 or 6850 redirects traffic to the InfoExpress CyberGatekeeper policy server and the remediation servers

4 InfoExpress CyberGatekeeper policy server receives HIC report from CyberGatekeeper Agent and informs the OmniSwitch 6400 or 6850 if the device has passed or failed

5 If HIC passed, OmniSwitch 6400 or 6850 selectively allows device traffic to production network following policy in user profile. If HIC failed, OmniSwitch 6400 or 6850 restricts traffic to remediation network only

Resident or on-demand agent continuous surveillance

Technical specifications

OmniSwitch products supporting HIC integration

Alcatel-Lucent OmniSwitch 6400 SGS and OmniSwitch 6850 SLS families with AOS, Release 6.3.4 or later

CGS-1000 CyberGatekeeper Server Appliance

- Hardware revision: 1000-sm1a
- Software revision: 6.02
- Compliance: RoHS, UL, FCC
- Power requirements: 5 A Max (100 V to 240 V 50/60 Hz, single power supply)
- Network interfaces: Dual 1000BT full duplex RJ-45 (copper)
- Audit connections: Rated up to 10,000 for policies with 500 audited conditions
- Enforcement modules:
  - ¬ CGSI (HIC): Max 100 client switches
  - ¬ EAP (RADIUS Proxy): Max 100 client switches
  - ¬ Dynamic NAC: Max 200 managed subnets
  - ¬ Bridge (in-line): Max 800 Mb/s (CGR-1000 dedicated bridge enforcement)

CGM CyberGatekeeper Manager Software Suite

- Includes Policy Manager and Reporting Server
- Requires Microsoft Windows 2003 Server® and Microsoft SQL Server® 2005/2008 database software
- Hardware specifications to support an implementation vary depending on total number of endpoints, policy complexity, and data retention period. The following sample configuration is provided only as a guide for supporting a 3000-endpoint implementation:

Web server (dedicated)

Windows 2003 Server SP1, IIS

- Processor and memory: Intel® Core™2 Quad 2.4 GHz, 3.0 GB of RAM
- Disk subsystem: RAID 5, 7200RPM disks, minimum 80 GB for OS and application

Database SQL server (dedicated)

Windows 2003 (64-bit) Server SP1, SQL Server 2005/2008

- Processor and memory: Intel Core 2 Quad 2.4 GHz, 8 GB of RAM
- Disk subsystem: RAID 5, 7200 RPM disks, minimum 100 GB for DB
- Expected average database size: 45 GB

OS6400-24, OS6400-P24, and OS6400-P24H

OS6400-48, OS6400-P48, and OS6400-P48H

OS6400-24U and OS6400-24UD

Non-PoE Models

OS6850-24
OS6850-24X
OS6850-48
OS6850-48X

PoE Models

OS6850-P24
OS6850-P24X
OS6850-P48
OS6850-P48X

Fiber Model

OS6850-U24X

www.alcatel-lucent.com

Alcatel·Lucent